Defense Message System (DMS)

Interim Procedure 7-V02

Firewall Policy

// Signed //
John W. Milton
Chief, DISN Messaging
DMS Global System Manager

IP Authority: David Tibbals
DISA 3121
DMS DN:
ou=DoD @ ou=DISA @ ou=Organizations @ ou=GOSC @ ou=ORG STAFF @ ou=OPS @ ou=DMS GSM
E-mail:
DMSGSM@ncr.disa.mil

Summary of Changes

Changed Table 1-1, from Port 17003 to Port 104 for X.500 DISP and X.500 DAP. Port 17003 was not correct. Port 104 is the correct port for these protocols.

Table of Contents

1 Purpose

The purpose of this document is to identify the operational impact of Military Service and Department of Defense Agency (S/a) implemented network firewalls on DMS protocols and provide the operational policy and procedures between the Regional Network Operations and Security Centers (RNOSC) and Area Control Centers and Local Control Centers (ACC/LCC) when firewalls limit full use of those protocols.

2 Applicability

This policy applies to DMS Area Control Centers and Local Control Centers (ACC/LCC).

3 Firewall Description

A firewall is used to establish a protected environment and encompasses all components within a protected enclave such as an agency's site. Firewall Reports 1-4 and the DMS Firewall Configuration Guidance document provides in-depth technical explanations and analysis of firewalls and their impact on the DMS. These documents are available in the DMS Online Library. The DMS Online Library is accessable through the DMS Controlled Access WEB Page at http://www.disa.mil/D2/dms/invited/. A password is required to access the site. Information on how to obtain a password is located on the DISA DMS Web Site at http://www.disa.mil/D2/dms/.

4 Local Firewall Implementation

Services and agencies implement firewalls in accordance with their own network security policy. However, when those firewalls are located between the local DMS enclave and the DMS backbone infrastructure, DMS operation and systems management can be affected. Figure 1-1 illustrates a common local network security policy implementation of a firewall, and shows the effect on DMS operations. However, some sites may be different.

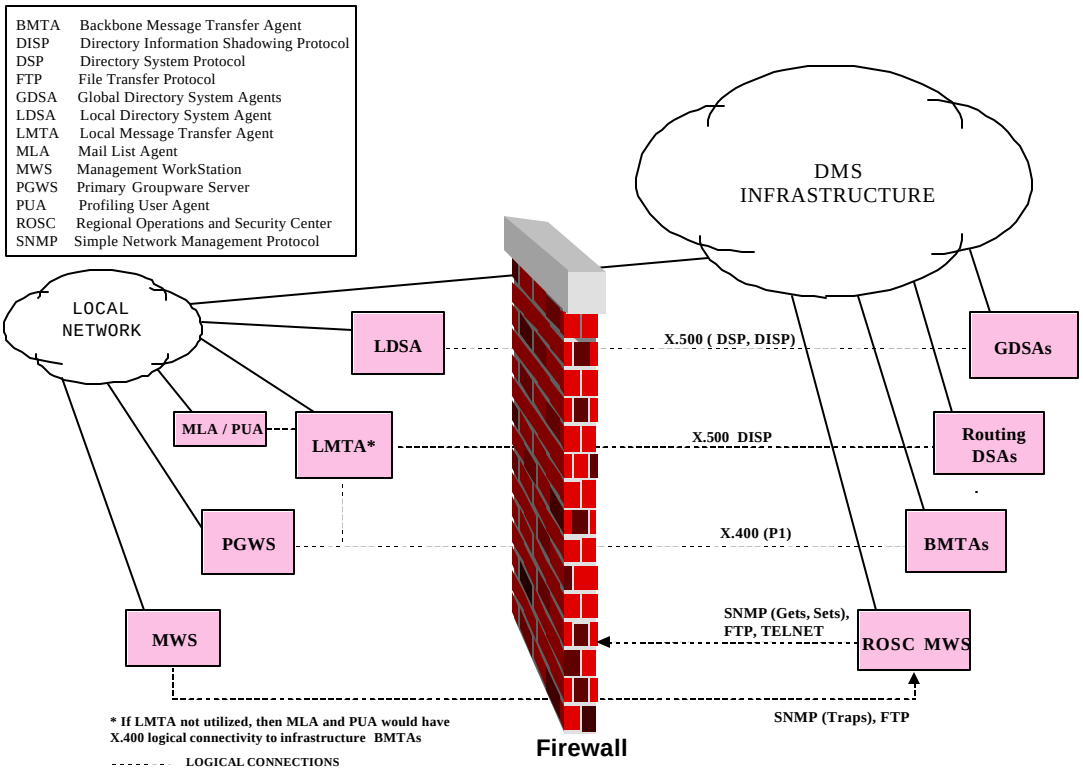

Figure 1-1 Common Local Network Firewall Implementation

5 Policy

DMS Area Systems Managers (ASM) and Local Systems Managers (LSM) will work with local network and/or firewall administrators to ensure that firewalls are configured to allow passing of X.400 and X.500 protocols for DMS organizational messaging and directory services. ASM/LSMs are expected to remain cognizant of the configuration of their local network firewall and the impact on DMS operation and management between the local site, the DMS backbone infrastructure, and the servicing RNOSC.

6 Protocols

Table 1-1, identifies the protocols and associated port utilized by DMS for messaging, directory services, system

management and control. It identifies the affected local components, affected regional components at the regional nodes and RNOSCs, and the function the protocol facilitates. The shaded rows indicate the protocols commonly blocked by local firewalls due to security concerns and policy. However, it is possible for other protocols to be blocked depending on the site's individual network security policy and firewall implementation.

PROTOCOL	LOCAL COMPONENT	REGIONAL COMPONENT	FUNCTION
X.400 P1 Port 102	PGWS LMTA MLA PUA	BMTA	Message Transfer
X.500 DSP DISP Port 17003	LDSA	RGDSA MGDSA SGDSA Master PLA DSA Shadow PLA DSA	Chaining Shadowing
X.500 DISP Port 104	LMTA	Domain (Shadow) Server/Routing DSA	RCDB Shadowing
X.500 DAP Port 104	LMTA	RNOSC-ADUA	Admin
FTP Locally Initiated Port 20 (Data) Port 21 (Control)	MWS	RNOSC-MWS	-Trouble Ticket Transfer -Messaging Reports -MWS Back-up Map/Hosts
FTP RNOSC Initiated Port 20 (Data) Port 21 (Control)	PGWS LMTA MLA PUA	RNOSC-MWS	Log Retrieval/ Message Trace
SNMP (Trap) Port 162	MWS PGWS LMTA	RNOSC-MWS	Monitor

PROTOCOL	LOCAL COMPONENT	REGIONAL COMPONENT	FUNCTION
	MLA PUA		
SNMP (Get/Set) Port 161 (Native HP-UX) Port 26017 (Agent) Port 6664/5 (Agt Factory)	MWS PGWS LMTA MLA PUA	RNOSC-MWS	Monitor and Control
NTP Port 123	PGWS LMTA MLA PUA LDSA MWS ADUA	BMTA SGDSA	Time Synchronization
Telnet Port 23	MWS	RNOSC-MWS	Configuration Control

Table 1-1 Firewall Protocol Table

7 Procedures

Procedures for each of the identified protocols blocked by a local firewall are as follows:

7.1 X.400, P1 Protocol

This protocol shall not be blocked by local firewalls.

7.2 X.500 DSP, DISP and DAP Protocols

These protocols shall not be blocked by local firewalls.

7.3 FTP Incoming

When the FTP protocol is blocked entering (e.g. RNOSC Management Work Station (MWS) to ACC/LCC MWS) the protected

enclave, the servicing RNOSC will not be able to retrieve log files from site components and subsequently be unable to perform a message trace to the site. In this situation the RNOSC will trace to the last BMTA on the message route and then pass a request for message trace continuation to the ACC/LCC. The procedures in the latest version of IP 2, Message Trace, apply.

7.4 FTP Outgoing

Normally, outgoing FTP (e.g. ACC/LCC MWS to RNOSC MWS) is not blocked, however, when it is, the site will be incapable of transferring trouble tickets and messaging reports to the RNOSC. In this event, trouble tickets will be forwarded via DMS operations message[1]. The message will contain all the information normally provided in a trouble ticket.

7.5 SNMP (Trap)

SNMP (Trap) is used for local component monitoring only and does not affect interoperability between the ACC/LCC and the RNOSC.

7.6 SNMP (Get/Set)

The SNMP (Get/Set) protocol is used by the RNOSC to monitor and control local components listed in Table 1-1. When this protocol is blocked the RNOSC will not be able to determine the status of local components if a problem occurs. In this situation the ASM/LSM is responsible to notify the RNOSC by operations message whenever one of the listed components is out-of-service.

7.7 NTP

[1] Operations Message - DMS organizational messages transferred between ACC/LCCs, DTHs and RNOSCs for the purpose of exchanging DMS operations related information. The Operations Message is established per DMS Interim Procedure 1, DMS Operations Coordination Messages.

NTP is normally used to establish time synchronization with an external component. When NTP is blocked by a local firewall, time may be obtained from a local component or filtered through the firewall to an external server. This is a local decision.

7.8 Telnet

Telnet sessions between the RNOSC and ACC/LCC components require strong authentication. This protocol is only used when FTP is not available through the MWS or other contingency situation. The RNOSC and ACC/LCC will coordinate the use of Telnet when it is required.